UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

CYBERGENETICS CORP.,

Plaintiff,

v.

INSTITUTE OF ENVIRONMENTAL SCIENCE AND RESEARCH and NICHEVISION, INC.,

Defendants.

Case No. 5:19-cv-001197-SL

Judge Sara Lioi

STIPULATED ORDER RELATING TO THE DISCOVERY OF ELECTRONICALLY STORED INFORMATION ("ESI")

The parties to this Stipulated ESI Order have agreed to the terms of this Order; it is ORDERED:

1. **<u>Introduction</u>.** Plaintiff, Cybergenetics Corp. ("Cybergenetics"), and Defendants, Institute of Environmental Science and Research ("ESR") and NicheVision, Inc. ("NicheVision"), adopt the following protocol relating to the discovery of electronically stored information in the above captioned proceedings, including any appeals thereto.

2. **<u>Discovery disclosures</u>.**

a. No later than seven (7) days after filing this protocol the parties shall exchange the following information:

(i) A list of the most likely custodians of relevant electronically stored information ("identified custodians"), including a brief description of each person's title, responsibilities, and current employment status.

(ii) The name of the individual who shall serve as that party's "e-discovery coordinator" (see ¶ 3).

b. No later than January 10, 2019, the parties shall exchange the following information:

(i) A list of each relevant electronic system that has been in place since October 1999 for Plaintiff and 2011 for Defendants and a general description of each system, including the nature, scope, character, organization, and formats employed in each system. The parties should also include other pertinent information about their electronically stored information and whether that electronically stored information is of limited accessibility. Electronically stored information of limited accessibility may include those created or used by electronic media no longer in use, maintained in redundant electronic storage media, or for which retrieval involves substantial cost.

(ii) The name of the individual designated by a party as being most knowledgeable regarding that party's electronic document retention policies ("the retention coordinator"), as well as a general description of the party's electronic document retention policies for the systems identified above (see ¶ 7).

(iii) Notice of any problems reasonably anticipated to arise in connection with e-discovery.

c. Where the “retention coordinator” of ¶ 2(a)(ii) or the “e-discovery coordinator” of ¶ 2(b)(ii) is a third-party consultant entity, reference to such coordinator(s) in this Protocol may be to the third-party consultant entity rather than to an individual.

d. No party needs to preserve or search for ESI from custodians or sources not identified by that party per ¶ 2(a)-(b), unless subsequently requested by opposing counsel in the course of discovery for good cause. A party failing to use good faith for the identification per ¶ 2(a)-(b) is subject to sanctions, including paying the other side’s attorney fees incurred as a result of the failure.

e. The following categories of ESI are not discoverable and need not be preserved:

(i) “deleted,” “slack,” “fragmented,” or “unallocated” data on hard drives or solid state drives;

(ii) random access memory (RAM) or other ephemeral data;

(iii) on-line access data such as temporary internet files, history, cache, cookies, etc.;

(iv) data in metadata fields that are frequently updated automatically, except as expressly required by Appendix A hereto for date last accessed and date last modified;

(v) backup data that is substantially duplicative of data that is more accessible elsewhere;

(vi) other forms of ESI not listed here whose preservation requires extraordinary affirmative measures that are not utilized in the ordinary course of business, in which case the party will disclose any such forms to all other parties as inaccessible ESI;

(vii) voicemail;

(viii) cloud-based social media;

(ix) ESI on cellular telephones, portable media players (e.g., iPod or MP3 player), handheld personal digital assistants (PDAs);

(x) ESI on tablets that is substantially duplicative of data that is more accessible elsewhere;

(xi) ESI filtered out by spam and/or virus filtering software, so long as the criteria underlying the filtering are reasonable;

(xii) server, system, or network logs; and

(xiii) system files (e.g., .EXE, .DLL, .SYS, etc.) not created for or provided with STRmix or TrueAllele (see also ¶ 6(f)(i)).

f. Nothing in this Section relieves a party from its obligation to preserve evidence it knows may be relevant to any party's claim or defense.

3. E-discovery coordinator. In order to promote communication and cooperation between the parties, each party shall designate a single individual through which all e-discovery requests and responses are coordinated ("the e-discovery coordinator"). Regardless of whether the e-discovery coordinator is an attorney (in-house or outside counsel), a third party consultant, or an employee of the party, he or she must be:

a. Familiar with the party's electronic systems and capabilities in order to explain these systems and answer relevant questions.

b. Knowledgeable about the technical aspects of e-discovery, including electronic document storage, organization, and format issues.

c. Prepared to participate in e-discovery dispute resolutions.

At all times, the attorneys of record shall be responsible for responding to e-discovery requests. However, the e-discovery coordinators shall be responsible for organizing each party's e-discovery efforts to insure consistency and thoroughness and, generally, to facilitate the e-discovery process. The ultimate responsibility for complying with e-discovery requests rests on the parties. Fed. R. Civ. P. 37(f).

4. **<u>Timing of e-discovery</u>.** Discovery of relevant electronically stored information shall proceed in a sequenced fashion.

a. After receiving requests for document production, the parties shall search their documents, other than those identified as limited accessibility electronically stored information, and produce relevant responsive electronically stored information in accordance with Fed. R. Civ. P. 26(b)(2).

b. Electronic searches of documents identified as of limited accessibility shall not be conducted until the initial electronic document search has been completed. Requests for information expected to be found in limited accessibility documents must be narrowly focused with some basis in fact supporting the request.

c. On-site inspections of electronic media under Fed. R. Civ. P. 34(b) shall not be permitted absent exceptional circumstances, where good cause and specific need have been demonstrated.

5. **<u>Search methodology</u>.** If a party intends to employ an electronic search, technology-assisted review, or similar technologies (e.g., predictive coding or advanced analytics, collectively “TAR Tools”) to locate relevant electronically stored information, the party will in good faith use a search methodology that the party believes will return a reasonably high proportion of responsive documents, and the party will log its search methodology. Neither party is entitled to the other’s search methodology, but disclosure of search methodology may be compelled by a showing of good cause.

6. Format.

a. TIFF/Native File Format Production. The default production format will be black-and-white Group IV single-page TIFF (300 DPI) with corresponding multi-page text and necessary load files. The load files will include an image load file as well as a metadata (.dat) file with the metadata fields identified below on the document level to the extent available. However, spreadsheets (e.g., Microsoft Excel), databases, audio files, videos, computer-aided design (CAD) files, and other files that do not render into image format consistently and presentation formats (e.g., Microsoft PowerPoint) shall be produced in their native form with a placeholder TIFF image stating “Document Produced Natively,” unless such files contain redactions, in which case the files will be produced in TIFF format. When converting an electronic document to a PDF or TIFF format, the producing party shall ensure that any track changes, markups, comments, notes (including notes in a Power Point or other presentation document), annotations, or similar features contained in the document are visibly displayed in the image generated from the file.

b. Database. If ESI stored in a database is responsive to a document production request, the producing party may respond to the request by producing a generated report of, or a usable export file with, the responsive ESI, and need not produce the entire database. Documents collected from databases not tied to an individual custodian will be identified by "DMS" or similar as the custodian.

c. Numbering/Endorsement. All produced Discoverable Information will have a unique Control ID assigned, regardless of the format of the Discoverable Information. The Control ID will be generated so as to identify the producing party. The Control ID will not include the full names of any parties. For Discoverable Information produced in TIFF image format, each TIFF image will have a legible, unique page identifier ("Bates Number") electronically "burned" onto the image at a location that is unlikely to obscure relevant information from the source document. A producing party should be consistent in the Bates Number prefixes it uses across its productions. In the case of materials deemed confidential in accordance with any applicable federal, state, or common law, or any protective order or confidentiality stipulation entered into by the parties, a confidentiality designation may be "burned" onto the document's image at a location that is unlikely to obscure relevant information from the source document. Should a Bates Number or confidentiality designation obscure information from the source document that the receiving party wishes to see, the receiving party may request the source document without such obscurement by identifying its Bates Number to the producing party and the producing party will promptly produce a substitute, unobscured document. This section is not intended to require a party to review all Bates-numbered materials prior to production.

d. Hard-copy Documents. Where practicable, hard-copy documents will be scanned and produced in electronic format by the producing party. Any such hard-copy documents produced in electronic format pursuant to this paragraph will be considered "Hard Copy" for purposes of complying with Appendix A hereto.

e. Metadata Fields and Processing.

(i) Metadata Fields: For email, the parties shall provide all applicable email metadata fields outlined in **Appendix A** and associated with each document produced, to the extent they are reasonably available from the source of collection. For non-email electronic documents (such as Microsoft Word), the parties shall provide all applicable non-email ESI metadata fields outlined in **Appendix A** and associated with each electronic document produced, to the extent they are reasonably available from the source of collection. For hard copy documents that are produced by a party (as opposed to being made available for inspection), the parties shall provide all applicable metadata fields associated with hard copy outlined in **Appendix A** for each document produced to the extent they are reasonably available.

(ii) Required Metadata: No party has an obligation to create or manually code metadata fields that are not automatically generated by the processing of the ESI or that do not exist as part of the original metadata of the electronic document, with the exception of the following as described in **Appendix A**: (a) BegBates, (b) EndBates, (c) Custodian, (d) Confidentiality, (e) OCR Path (f) Producing Party; (g) Production Volume, and (h) Redacted (y/n), which should be populated regardless of whether the fields can be populated pursuant to an automated process.

(iii) Time Zone: ESI items shall be processed in a manner that preserves their existing time, date, and time-zone metadata (e.g., the email of a Document Custodian located in Pennsylvania will be processed as Eastern Time, while a Document Custodian located in California will be processed as West Coast Time). If GMT time zone is used, then a time-zone offset metadata field must be provided indicating the original time zone in which the custodian of the document received or authored the document.

(iv) Searchable Text File Specifications. Each party shall provide fully searchable text files. Extracted text should be included for all records, with the exception of those records that originated as hard copy or redacted documents or those records where text cannot be extracted. For hard copy documents, OCR text will be provided. For redacted documents, OCR text for the redacted version will be provided. Text must be produced as separate text files, not as fields within the .DAT file. The full path to the text file should be included in the .DAT file.

f. Pre-Production Filtering. To the extent reasonably feasible, the parties will comply with the following:

(i) Deduplication: A producing party shall use commercially reasonable efforts to globally de-duplicate (across custodians) identical ESI within their own productions, based upon a commercially accepted method (e.g., MD5 or SHA-1 hash values).

(ii) De-NISTing. Electronic file collections will be De-NISTed, removing commercially available operating system and application file information contained on the current NIST file list.

(iii) Zero-byte Files. The parties shall filter out stand-alone files identified as zero-bytes in size.

(iv) Email Threading. The Parties may use "email thread suppression." To the extent a Party uses email thread suppression, the Party will make reasonable efforts to produce a unique thread identifier for each thread, which will correlate two emails that have been identified to be part of the same thread, but that do not meet the criteria described in this paragraph of having a derivative email that fully represents a previous email. As used in this Protocol, email thread suppression means reducing duplicative production of email threads by producing the most inclusive email containing the thread of emails, as well as all attachments within the thread, and excluding emails constituting duplicates of emails within the produced string. For purposes of this paragraph, only email messages in which the parent document and all attachments are exactly the same will be considered duplicates. Duplicative emails suppressed under this paragraph need not be reflected on the Party's privilege log. Should a receiving party wish to see any individual email within an inclusive email thread, the receiving party may request the individual email within the inclusive email by identifying its Bates Number, date, and time to the producing party and the producing party will promptly produce the included individual email.

g. Native Files. After initial production in image file format is complete, a party must demonstrate particularized need for production of electronically stored information in their native format.

h. Redactions: The parties agree that where ESI items need to be redacted, they shall be produced solely in TIFF with each redaction clearly indicated. Any unaffected data fields specified in **Appendix A** shall be provided. For example, if attorney-client privilege requires that the Subject field of a document needs to be redacted, all other available data fields specified in **Appendix A** shall be provided.

i. Variations to Production Format. In certain circumstances, variations to the production format specified in this Protocol may be necessary. In such circumstances, the parties will meet and confer regarding the Production Format.

7. Retention. By no later than seven (7) days after filing this protocol, the parties will disclose the steps each party has taken to segregate and preserve the integrity of all relevant electronically stored information. At a minimum, the retention coordinators shall take steps to ensure that relevant e-mail of identified custodians shall not be permanently deleted in the ordinary course of business and that relevant electronically stored information maintained by the individual custodians shall not be altered. By no later than fourteen (14) days after filing this protocol, each party's counsel shall file a statement of compliance with the court that the above procedures have been implemented.

8. **Privilege.** Electronically stored information that contains privileged information or attorney-work product shall be governed by Federal Rule of Civil Procedure 26(b)(5)(B) and any relevant provisions of any Protective Order entered in this case. Pursuant to Federal Rule of Evidence 502(d), the production or inspection of documents that a producing party claims was inadvertent and should not have been produced or disclosed because of the attorney-client privilege, the work product immunity, or any other applicable privilege or immunity from discovery is not and shall not be deemed to be a waiver of any such privilege or immunity to which the party producing documents would have been entitled had the documents not inadvertently been produced or disclosed. The use of privilege metadata and search term screening and/or TAR Tools are reasonable measures to protect against the disclosure of privilege information.

9. **Privilege Logs**. Each party shall use good faith efforts in determining the reasonable technology and processes to identify and log privileged Discoverable Information.

a. No party is required to list on a privilege log information generated on or after May 24, 2019, if privileged or protected as work product, absent a showing of good cause.

b. If a producing party identifies portions of Discoverable Information that are privileged and redacts such portions of the Discoverable Information on that basis, the producing party must log the fact of redaction, provided however that a party need not provide a log entry where the face of the redacted Discoverable Information provides the information that otherwise would appear on a log.

c. For each privileged or work-product-protected ("Protected") email chain, the disclosing party may provide the required privilege-log information for the top (i.e., most recent) email in the email chain and also list the total number of emails in that chain, which may be based on the Conversation Index of that chain. An "email chain" as used in this paragraph means a single file that contains multiple emails sequentially in the body of the file (e.g., forwards or replies), not separate files that contain emails related in the same conversation. If one Protected email chain is subsumed within another, larger Protected email chain, both email chains will be logged. This section does not relieve a party from producing any non-Protected emails within a Protected email chain.

10. **<u>Costs</u>.** The court will apportion the costs of electronic discovery upon a showing of good cause, in accordance with Federal Rule of Civil Procedure 26(c)(1)(B).

11. **<u>Discoverability and Admissibility</u>**. Nothing in this Protocol shall be construed to affect the admissibility of Discoverable Information. All objections to the discoverability or admissibility of any Discoverable Information are preserved and may be asserted at any time.

12. **<u>Discovery Requests</u>**. With each issued interrogatory; request for production of documents, ESI, or things; or request for admission, per Federal Rules of Civil Procedure 33, 34, or 36, the party seeking discovery will provide a copy of the interrogatory, request for production, or request for admission in an editable, Microsoft Word format to facilitate responses.

13. **<u>Modification</u>**. Any practice or procedure set forth herein may be varied by agreement of the parties, which will be confirmed in writing, where such variance is deemed appropriate to facilitate the timely and economical exchange of Discoverable Information. Any party that seeks to deviate from or exceed the discovery parameters set forth herein, must obtain leave of Court to do so unless all parties otherwise consent in writing. Before seeking Court intervention, the parties shall meet and confer in good faith regarding any modification.

IT IS SO ORDERED.

Date: ____________

____
HONORABLE SARA LIOI
U.S. DISTRICT JUDGE

STIPULATED TO BY THE PARTIES:

[Effective Date when filed with the Court]

/s/ Mark M. Supko

Counsel for Plaintiff

/s/ John M. Skeriotis

Counsel for Defendant

Dated: December 23, 2019

/s/ Mark M. Supko
Mark M. Supko (admitted *pro hac vice*)
Siri M. Rao (admitted *pro hac vice*)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington, DC 20004
Telephone: (202) 624-2500
Facsimile: (202) 628-5116
msupko@crowell.com

Pilar R. Stillwater (admitted *pro hac vice*)
CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111
Telephone: (415) 986-2800
Facsimile: (415) 986-2827
pstillwater@crowell.com

Michael J. Garvin (0025394)
VORYS, SATER, SEYMOUR
and PEASE LLP
200 Public Square
Suite 1400
Cleveland, Ohio 44114
Telephone: (216) 479-6100
Facsimile: (216) 479-6060
mjgarvin@vorys.com

Attorneys for Cybergenetics Corp.

/s/ John M. Skeriotis

John M. Skeriotis (Ohio Bar # 0069263)
jms@etblaw.com
Sergey Vernyuk (Ohio Bar # 0089101)
sv@etblaw.com
EMERSON THOMSON BENNETT, LLC
1914 Akron-Peninsula Rd.
Akron, OH 44313
Telephone: (330) 434-9999
Facsimile: (330) 434-8888

Attorneys for Defendants Institute of Environmental Science and Research Limited and NicheVision Inc.

APPENDIX A: REQUIRED METADATA FIELDS

Field	Description	Email	Non- Email ESI	Hard Copy
Bates Number Begin	Beginning page Bates number	x	x	x
Bates Number End	Ending page Bates number	x	x	x
BeginAttachment	Beginning production # of parent in a family	x	x	
EndAttachment	Ending production # of last page of the last attachment in a family	x	x	
Attachment Count	Number of attachments to an email	x	x	
Family Range	Beginning page of parent document and ending page of attachment range	x	x	
Custodian	Custodian that possessed the document or electronic file.	x	x	x
AllCustodians	All production custodians or non-human production data sources associated with the produced document	x	x	
File Name	File name of document		x	
File Extension	File extension of document		x	
File Size	File size in bytes	x	x	x
Page Count	For documents produced in TIFF form, number of pages in the document. For documents produced in native, page count will be 1 (for placeholder).	x	x	x
Email Subject	Subject of email	x		
Author	Document author		x	
From	Email author	x		
To	Email recipients	x		
CC	Email copyees	x		
BCC	Email blind copyees	x		
Message ID	Email unique identifier	x		
Importance	Email importance flag	x		
Date Sent	Date sent (per ¶ 6(c)(iii))	x		
Time Sent	Time sent (per ¶ 6(c)(iii))	x		

Field	**Description**	**Email**	**Non- Email ESI**	**Hard Copy**
Date Received	Date received (per ¶ 6(c)(iii))	x		
Time Received	Time received (per ¶ 6(c)(iii))	x		
Date Created	Date created (per ¶ 6(c)(iii))		x	
Date Modified	Date last modified (per ¶ 6(c)(iii))		x	
Date Accessed	Date last accessed (per ¶ 6(c)(iii))		x	
Hash Value (MD5 or SHA-1)	Unique electronic signature of email or electronic file	x	x	
Email Thread Family ID	Unique identifier from email threading algorithm to denote emails from a single thread and all attachments (if using email thread suppression); also known as Conversation Index	x		
Password Protection/ Encryption	Descriptor for documents that are password-protected or encrypted (<yes> or <no>)	x	x	
Production Volume	Production volume name	x	x	x
Confidentiality	Confidentiality designation pursuant to the Stipulated Protective Order.	x	x	x
Redacted	Descriptor for documents that have been redacted (<yes> or <no>)	x	x	x
Timezone	Timezone the data was processed in	x	x	
Nativelink	Path and filename for the native file on production media: Natives\001\001\ABC00000001 .XLSX	x	x	
Textpath	Path to *.txt file containing extracted or OCR text; Text\001\001\ABC00000001-txt	x	x	x